WHAT IS CLAIMED IS:

1. A method for evaluating the random numbers generated by a random number, the method comprising the steps of:

generating a stream of random numbers;

determining an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals;

applying each of the average number of bits indicative of said predetermined logic value to an exponential averaging operation (A); and,

determining whether said generated random numbers are unpredictable by comparing the output of said exponential averaging operation (A) to a predetermined acceptance range.

2. The method of claim 1, wherein the value of said predetermined logic value is one of 1's and 0's.

3. The method of claim 1, further comprising the step of determining that said generated random numbers are predictable when the output of said exponential averaging operation (A) falls outside said predetermined acceptance range.

4. The method of claim 1, further comprising the step of notifying that said generated random sequences are predictable when the output of said exponential averaging operations (A) falls outside said predetermined acceptance range.

5. The method of claim 1, further comprising the step of updating all said exponential averaging operations (A) each time a new bit is generated.

6. The method of claim 5, wherein said exponential averaging operation (A) is updated according to the following equation:

$$A_{new} = \alpha \cdot A_{old} + b,$$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$), and wherein b is a value comprising 1 when the average number of bits is obtained, otherwise 0.

7. The method of claim 1, further comprising the step of generating a new set of random sequences when the output of said exponential averaging operation falls outside said predetermined acceptance range.

8. The method of claim 6, wherein said predetermined acceptance range is defined as follows:

$$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$$

where c is selected to achieve a desired security threshold level.

9. A method for evaluating the random numbers generated by a random number, the method comprising the steps of:

(a) generating a stream of random numbers of binary bits using said random number generator;

(b) determining an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals;

(c) computing an exponential averaging operation (A) on the average number of bits indicative of said predetermined logic value;

(d) comparing the output of said exponential averaging operation (A) to a predetermined acceptance range; and,

(e) determining that said generated random numbers are predictable when the output of said computed exponential averaging operation (A) falls outside said predetermined acceptance range.

10. The method of claim 9, further comprising the step of:

repeating said steps (a) - (e) until said computed exponential averaging operation (A) repeatedly falls outside said predetermined acceptance range more than a predefined number of times.

11. The method of claim 9, further comprising the step of notifying that non-random numbers are generated when said computed exponential averaging operation (A)

repeatedly falls outside said predetermined acceptance range more than a predefined number of times.

12. The method of claim 9, further comprising the step of generating a new set of random numbers when said computed exponential averaging operation (A) repeatedly falls outside said predetermined acceptance range more than a predefined number of times.

13. The method of claim 9, further comprising the step of updating said exponential averaging operation (A) according to the following equation:

$$A_{new} = \alpha \cdot A_{old} + b,$$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$), and wherein b is a value comprising 1 when the average number of bits is obtained, otherwise 0.

14. The method of claim 13, wherein said predetermined acceptance range is defined as follows:

$$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$$

where c is selected to achieve a desired security threshold level.

15. An apparatus for evaluating the random numbers generated by a random number, comprising:

a random generator unit for generating substantially random sequences of binary bits;

a detector unit, coupled to the output of said random generator unit, for detecting whether said generated random sequences are unpredictable; and,

a switching unit, coupled to the outputs said random generator unit and said detector unit, for disabling the flow of said generated random sequences for a subsequent application when said generated random sequences are determined to be predictable,

wherein an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals is determined and applied to exponential averaging operations (A) and wherein, if the output of said exponential averaging operations (A) falls outside a predetermined acceptance range, determining that said generated random sequences are predictable.

16. The apparatus of claim 15, further comprising means for transmitting an alarm signal when the output of said exponential averaging operation (A) falls outside said predetermined acceptance range.

17. The apparatus of claim 15, wherein said exponential averaging operation (A) is performed according to the following equation:

$$A_{new} = \alpha \cdot A_{old} + b,$$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$), and wherein b is a value comprising 1 when the average number of bits is obtained, otherwise 0.

18. The apparatus of claim 17, wherein said predetermined acceptance range is defined as follows:

$$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$$

where c is selected to achieve a desired security threshold level.

19. A machine-readable medium having stored thereon data representing sequences of instructions, and the sequences of instructions which, when executed by a processor, cause the processor to:

generate a stream of random bits;

determine an average number of bits that have a value of a predetermined logic value at a specific, predefined range of intervals;

perform an exponential averaging operation (A) on the number of bits indicative of said predetermined logic value; and,

compare the output of said exponential averaging operations (A) to a predetermined acceptance range.

20. The machine-readable medium of claim 19, wherein said generated random numbers are determined to be predictable when said computed exponential averaging operation (A) falls outside said predetermined acceptance range.

21. The machine-readable medium of claim 19, wherein said exponential averaging operation (A) is performed according to the following equation:

$$A_{new} = \alpha \cdot A_{old} + b,$$

wherein $\alpha = 1 - 1/n$, and α falls between 0 and 1 ($0 < \alpha < 1$), and wherein b is a value comprising 1 when the average number of bits is obtained, otherwise 0.

22. The machine-readable medium of claim 21, wherein said predetermined acceptance range is defined as follows:

$$[n/2 - c \cdot \sqrt{n}, n/2 + c \cdot \sqrt{n}],$$

where c is selected to achieve a desired security threshold level.